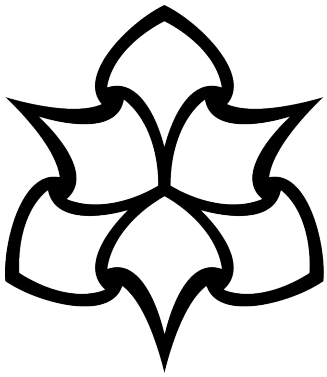

Efficient and Secured Swarm Pattern Multi-UAV Communication

[1]Gunasekaran Raja, *Senior Member, IEEE*, [2]Sudha Anbalagan, [3]Aishwarya Ganapathisubramaniyan, [4]Ali Kashif Bashir, *Senior Member, IEEE*, [5]Madhumitha Sri Selvakumar, [6]Shahid Mumtaz, *Senior Member, IEEE*

***Abstract*–Unmanned Aerial Vehicle (UAV) or drone, is an evolving technology in today's market with an enormous number of applications. Mini UAVs are developed in order to compensate the performance constraints imposed by larger UAVs during emergency situations. Multiple mini autonomous UAVs require communication and coordination for ubiquitous coverage and relaying during deployment. Multi-UAV coordination or swarm optimization is required for reliable connectivity among UAVs, due to its high mobility and dynamic topology. In this paper, a Secured UAV (S-UAV) model is proposed which takes the location of the UAVs as inputs to form a Wireless Mesh Network (WMN) among multiple drones with the help of a centralized controller. After WMN formation, efficient communication takes place using A* search, an intelligent algorithm that finds the shortest communication path among UAVs. Further, the S-UAV model utilizes cryptographic techniques such as Advanced Encryption Standard (AES) and Blowfish to overcome the security attacks efficiently. Simulation results show that the S-UAV model offers higher throughput, reduced power consumption and guaranteed message transmission with reduced encryption and decryption time.**

***Index Terms*—Unmanned Aerial Vehicle, Swarm Optimization, Wireless Mesh Networks, A* Search, Blowfish, Advanced Encryption Standard**

I. Introduction

In Wireless networks, Mobile Ad hoc NETwork (MANET) is a dynamically self-organizing network consisting of mobile nodes where communication takes place through wireless links such as IEEE 802.11 a/b/g/n. Later on, these mobile nodes were embedded in moving vehicles as termed as Vehicular Ad hoc Network (VANET) and aerial vehicles, resulting in Flying Ad hoc Network (FANET). Unmanned Aerial Vehicle (UAV) is one of the categories of FANET.

UAV is a remote controlled or autonomous flying object. UAVs are used in military, civil and commercial applications at metro cities like inspection, aerial photography, earth monitoring, security, emergency response and so on [1]. Apart from the general flight instruments, UAVs are also equipped with a Global Positioning System (GPS), gyroscope and a distance sensor to safeguard the lives of people in an emergency situation. To ensure effective communication among multiple UAVs, the Internet of Drones (IoD) environment is developed. There are two types of UAV communications: UAV-to-UAV communication, where two UAVs communicate directly or with the help of multi-hop communication, and UAV-to-infrastructure communication where UAVs communicate with the BS and act accordingly. In either case, communication is a challenging issue as it depends on the data rate and its performance [2].

The communication in a UAV environment is adversely affected by its dynamic nature. In order to overcome the dynamic nature, different types of antennas are used. UAVs use an omnidirectional antenna, operating on the 2.4 GHz band in order to ensure uniform distribution of radio power in the horizontal direction. To identify the direction, directional antennas are used which has an altitude of range 50 meters [3].

The key challenges in multi-UAV coordination and communication are, initially setting up communication over a large UAV environment is easy but expensive and hazardous to human life.Secondly, due to UAV's high mobility feature, the challenge is to efficiently communicate and coordinate among themselves [4], [5]. Finally, Swarm optimization in the UAV environment is vulnerable to attacks due to the enormous levels of wireless transmission and reception required. Potential attacks include GPS spoofing, de authentication attack, intercept data feed attack, virus attack, video replay attack and the data stream jamming attack [6], [7]. The proposed Secured UAV (S-UAV) model has the contributions to address the above challenges and as follows,

- To overcome the drawback of large UAVs, mini UAVs were developed with lower cost, smaller size and reduced weight [8]. Due to the smaller size of mini UAVs, they are less trackable compared to the larger UAVs.
- A coordinated multiple UAV environment is formed to achieve high level goals.In case of hardware failure in a single UAV environment, the UAV returns to the ground, whereas in a multi-UAV environment,UAVs can parallelize tasks and thus reduce the completion time of the task and results in improving the fault

Gunasekaran Raja and Madhumitha Sri Selvakumar are with NGNLab, Department of Computer Technology, Anna University, Chennai, India. (e-mail: dr.r.gunasekaran@ieee.org; smadhumithasri1998@gmail.com).

Sudha Anbalagan is with School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India. (e-mail: sudha.anbazhagan@gmail.com)

Aishwarya Ganapathisubramaniyan is with Foreign Exchange and Local Markets Group, Citicorp Services India Private Ltd., Chennai, India. (e-mail: aishwarya97.mit@gmail.com)

Ali Kashif Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, UK. (e-mail: dr.alikashif.b@ieee.org).

Shahid Mumtaz is with Instituto de Telecomunicações, Aveiro, Portugal. (e-mail: smumtaz@av.it.pt)

tolerance to a greater extent.
- In the proposed S-UAV model, Swarm optimization is used by building a Wireless Mesh Network (WMN) for UAV communication and coordination. To incorporate a swarm pattern in a multi-UAV environment, an intelligent A* search algorithm is established.
- For efficient route discovery, initially, UAV-to-controller communication takes place for WMN formation among active UAVs followed by UAV-to-UAV communication with the help of A* algorithm. A* finds the optimal path by excluding the obstacles between source and goal node.
- A secure authentication and key agreement scheme is proposed with the help of efficient cryptographic techniques such as AES and Blowfish, to overcome the vulnerable attacks in the UAV environment.

The rest of this paper is organized as follows: Section II provides a brief introduction to prior work in the fields of drone communication and coordination in WMN, UAV attacks and the proposed solutions. The system model of the proposed work with the explanation is given in section III. Efficient route discovery by finding the shortest path using A* algorithm and security algorithms to overcome the attacks are discussed in section IV. Finally, results and performance analysis are examined in Section V followed by a conclusion in Section VI.

II. Literature Survey

In this section, the drone communication and attacks encountered in the UAV environment are subjected to a survey. The current security algorithms in place to overcome these attacks are also discussed in detail.

Every UAV is an autonomous and programmable device that collaborates with other UAVs and takes intelligent decisions using a preloaded set of rules. UAV is structured as Centralized, Decentralized, Multigroup UAV and Multilayer UAV. Multilayer UAV is used for heterogeneous communication [9] and decentralized UAV is used for homogeneous communication [10]. The requirements and limitations of each of the wireless protocols for UAV communication are analysed in [11]. The spectra needed for UAV communication are analysed by the authors in [12] and it is also to be noted that the cellular and unlicensed spectrum is unsuitable for UAV imagery transmission. Since the spectra are designed for the terrestrial system, congestion will occur if the spectra are used for imagery transmission [13].

Much research has been undertaken to find a suitable network that can adapt to the dynamic nature and high mobility required by multi-UAV communication. The authors in [14] used Dijkstra and BFS algorithm for route discovery in multi-UAV. For drone swarm communication, WMN is suitable as it can configure itself automatically when a topology change occurs [15], [16]. The performance of different routing protocols used in WMN is analysed and their results show that Hybrid Wireless Mesh Protocol (HWMP) is suitable for FANET in terms of packet delivery, end to end delay and throughput [17], [18].

Further, the authors in [19] present a detailed survey on cybersecurity attacks against UAVs. The most frequently occurring attacks in UAVs are GPS jamming, GPS spoofing, zero-day vulnerabilities, de-authentication, intercept data feed attack and virus attack. The authors in [20] discussed the communication model and security requirements of UAVs. They also analysed how GPS spoofing and de-authentication can be performed in the UAV environment [21], [22].

The authors in [23] perform an attack on a drone and Ground Control Station (GCS) by using a drone simulator. The drone simulator mimics the action of GCS by performing neutralizing attacks between drones and GCS by knowing its weakness. The drone uses a waypoint protocol procedure to receive mission-related information from GCS. Based on the received information from the drone like GPS, the GCS decides whether the drone is working normally or not. If the attacker sends false mission information to the drone and false GPS information to the GCS both are neutralized. By using Homomorphic Encryption (HE), the risk of secret key management in the controller is removed and the encryption and decryption of data in the controller were effectively avoided, but HE does not ensure secure authentication [24].

Another major security vulnerability in drone communication is the low strength of GPS signals. This makes GPS as a target for attackers. The authors in [25] uses the Kalman filtering quadratic equation to determine the quality of incoming GPS signals to overcome GPS spoofing and GPS jamming attack. The authors also compared the communication overhead, computation overhead, functionality and security features under different schemes [26].

For secure authentication between two drones, temporal identity is exchanged to establish the secret key for their communication by using a Symmetric bivariate polynomial equation. By analyzing the impacts of security features in the traditional method, we have built a S-UAV model that uses A* algorithm for route discovery in the multi-UAV environment. A Secured authentication algorithm is also deployed to overcome impersonation, GPS spoofing, intercept data feed, impersonation and de-authentication in multi-UAV communication.

III. System Model

A geographical region is considered for the proposed S-UAV approach, by deploying UAVs which has a coverage area of about 200 km. The task of the UAV is to monitor the area and transmit the collected information to BS. There exist two groups of UAVs: UAV_G_1 and UAV_G_2. Initially, UAV_G_1 gets deployed at 't' time in the space which has the direct communication with the controller. After 't+x' time, where 'x' is chosen as a random number, UAV_G_2 gets deployed such that each UAV_G_2 can communicate with the controller with the help of UAV_G_1 forming an indirect routing between UAV_G_2 and the controller. Both

the group of UAVs get their mission related information and user control from the BS. Here, the routing decision is made by the controller for communication between the UAVs. The pictographic view of the S-UAV communication model and architecture is shown in Fig. 1.

IV. Proposed S-UAV Model

A. Efficient Communication

In the proposed S-UAV model, UAV-to-controller communication takes place initially for efficient formation of WMN among the active UAVs. Further, this is followed by UAV-to-UAV communication with the help of A* algorithm for efficient routing.

1) UAV-to-Controller Communication

The communication between UAV and controller takes place to establish the network. Initially, each UAV sends an active signal to indicate its presence. Along with the active signal, each UAV sends its latitude, longitude and altitude information to the controller. After receiving this information, the controller establishes a WMN topology among the active drones. The steps involved in WMN formation is represented in the flowchart shown in Fig. 2.

The controller establishes the WMN based on the distance between each UAV. Since distance is calculated based on the cartesian coordinates of the UAV, the controller converts the latitude L_1, longitude L_2 and altitude A of each UAV to two dimensional cartesian coordinate (X, Y) using Eq. (1) and Eq. (2).

$$X = (PN + A)\cos(L_1)\cos(L_2) \tag{1}$$

$$Y = (PN + A)\cos(L_1)\sin(L_2) \tag{2}$$

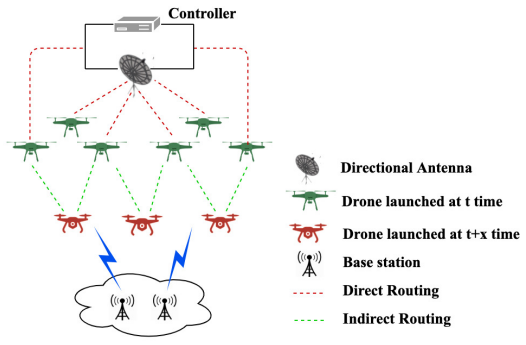

Fig. 1: S-UAV Communication Model

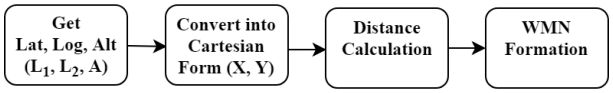

Fig. 2: Steps for WMN Formation

PN is the Prime Vertical Radius of Curvature and it is calculated as follows,

$$PN = a^2/\sqrt{a^2\cos^2(L_1) + b^2\sin^2(L_2)} \tag{3}$$

Where a= Semi-major axis (Equatorial radius)
b= Semi-minor axis (Polar radius)

2) UAV-to-UAV Communication

In UAV-to-UAV communication, a case where the power of a UAV is fully drained and it has quickly entered a dead state is considered. Before entering a dead state, the UAV has to transmit the mission related information it has collected so far to the BS as fast as possible. In a short period of time, the UAV has to search for the BS and pass on its information; however, this is not possible in most cases because searching operation takes more time and the UAV has to remain alive until acknowledgment returns from the BS. In this situation, the source UAV finds the shortest neighbour UAV to pass the information to, and the source UAV receives acknowledgment from the nearest neighbour UAV to ensure that the information will reach the BS without compromising integrity and confidentiality.

For the fastest and most efficient route discovery in multi-UAV communication, A*, an informed or heuristic search approach is modelled, which is widely used in gaming applications. A* finds the optimal path by excluding the obstacles between source and goal node. However, A* is the most popular choice for finding the shortest path and as it's a heuristic function which varies dynamically depending the on the nature of the problem. The Heuristic function h(n) is used to speed up the process and is used to calculate the cost of the optimal path between two nodes. The value of h(n) can either be an exact or an approximate value. Deriving an approximate value of h(n) takes less time than obtaining the exact value. The approximate value of h(n) can be obtained by any of the three ways such as, Manhattan distance, Euclidean distance and diagonal distance [27] which are expressed in equations (4), (5) and (6).

$$h(UAV) = (|UAV.x| - |UAV\_D.x|) + (|UAV.y| - |UAV\_D.y|) \tag{4}$$

$$h(UAV) = \sqrt{((UAV.x - UAV\_D.x)^2)} + \sqrt{((UAV.y - UAV\_D.y)^2)} \tag{5}$$

$$h(UAV) = max\{(|UAV.x| - |UAV\_D.x|), (|UAV.y| - |UAV\_D.y|)\} \tag{6}$$

Here x and y are the location of the UAV and `UAV_D` is the destination UAV.

For finding the best path using A* search algorithm, a weighted graph is constructed where each node represents the UAV, and weight between the nodes (edges) represents the distance between the UAVs. A* algorithm uses three functions to find the optimal path: g-function g(n) is an

incremental cost from the source node to each node, h-function or heuristic function h(n) is calculated for each UAV before reaching the destination and f-function or evaluation function f(n) is the addition of g(n) and h(n) where n denotes the particular UAV in the specified region. The node with the smallest f(n) is first included in the path map. The parameter g(n) is formulated as given in the Eq. (7).

$$g(UAV) = g(UAV\_Parent) + distance(UAV\_Parent, UAV) \quad (7)$$

From equation (4), (5), (6) and (7), f(n) is calculated as given in equation (8).

$$f(UAV) = g(UAV) + h(UAV) \quad (8)$$

3) Analysis of Communication Path

In this section, a region of multiple sender and receiver UAVs that communicate at the same time is taken into consideration. There is a possible of mutual interference while finding the shortest path. To circumvent the interference issue, instead of supplying the entire region as an input to A*, the S-UAV model finds the shortest path by excluding paths with mutual interference. This reduces the time complexity of the scanning process of the A* algorithm. Hence the efficiency of the A* search method is improved and the mutual interference problem is also solved.

Let us consider a region as a grid of size of 3*3 in a mesh network with 9 drones labeled from D_1 to D_9 in Fig. 3. The conditions for finding mutual interference path are,

- Criteria for two sender drones at the same time.
- Criteria for two receiver drones at the same time.
- Criteria for a drones to be receiver in the coexistence link.

As stated before, if a drone loses its energy, it needs to send data and receive an acknowledgment from the neighbour drones before entering into the dead state. To find the nearest neighbour, Hop Distance (HD) is used as a metric to find the mathematical relation for the above criterias. The distance between each drone is the same as the minimum number of hops between them.

A drone D_1 at position (x,y) is considered. The possible positions of drones to be the neighbour of D_1 are given in the Neighbour Set (N) as follows,

N = {(x-1,y-1), (x-1,y), (x-1,y+1), (x,y-1), (x,y+1),

$$(x+1, y), (x+1, y+1)\} \quad (9)$$

For each sender drone, the hop distance is calculated for each member in the set N based on its position. Let us consider two drones Source (S) and Destination (D) with positions (x_1, y_1) and (x_2,y_2) respectively. The HD between the two drones can be calculated using the Eq. (10) as follows:

$$HD = \frac{|x_1 - x_2| + |y_1 - y_2|}{2} \quad (10)$$

To calculate the number of possible paths between S and D, the Minimum Correct Direction (MCD) between S and D need to be obtained.

$$MCD = min\{|x_1 - x_2| + |y_1 - y_2|\} \quad (11)$$

From equation (12) the number of paths between S and D, P(S,D) is given by,

$$f(x) = \begin{cases} 1, if MCD = 0 \\ MCD + 1, if MCD = 1 \\ ((MCD + 1) * (MCD + 2))/2, if MCD = 2 \end{cases} \quad (12)$$

Further, the condition for the criteria based on HD to find the mutual interference path is derived in the following section.

Criteria for two sender drone at same time:

Here, three drones D_1, D_2 and D_3 are considered from Fig. 3 having positions (x_1, y_1), (x_2, y_2) and (x_3, y_3) respectively. The Neighbour (N) of D_1, D_2 and D_3 is given by,

$$N(D_1) = \{D_2, D_4, D_5\}$$
$$N(D_2) = \{D_1, D_3, D_4, D_5, D_6\}$$
$$N(D_3) = \{D_2, D_5, D_6\}$$

If both D_1 and D_2 act as a sender at the same time, then mutual interference occurs because both are the neighbours of each other. Similarly, D_2 and D_3 cannot act as a sender at the same time; however, D_1 and D_3 may act as sender simultaneously as they are not in the neighbour set of each other and mutual interference does not occur between D_1 and D_3. For any two drones to act as senders simultaneously, they should not be the neighbours of each other.

The criteria for drones D_1 and D_3 to be senders at the same time is obtained by finding the hop distances (D_1, D_2), (D_1, D_3) and (D_2, D_3) in relation to Eq. (10).

$$HD(D_1, D_2) = ((|x_1 - x_2| + |y_1 - y_2|)/2) = 1$$
$$HD(D_1, D_3) = ((|x_1 - x_3| + |y_1 - y_3|)/2) = 2$$
$$HD(D_2, D_3) = ((|x_2 - x_3| + |y_2 - y_3|)/2) = 1$$

The relation between HD and the Neighbour Set of drones D_1, D_2 and D_3 proves that, the two drones will act as sender simultaneously only if they are separated by at least two hop distances. This condition is expressed in equation (13).

$$HD(D_i, D_j) = ((|x_i - x_j| + |y_i - y_j|)/2) \geq 2, i \neq j \quad (13)$$

Criteria for two receivers at the same time:

The criteria of two receiver drones at the same time is analysed using the same Neighbour set (N) and HD of D_1, D_2 and D_3. The receiver drone will not perform the

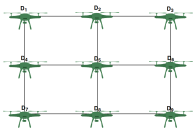

Fig. 3: Grid Mesh Network of Size 3*3

forwarding operations, two neighbour drones can act as a receiver at the same time. Therefore two drones will be the receiver simultaneously only if they are separated by at least one hop distance apart which is expressed as given in equation (14).

$$HD(D_i, D_j) = ((|x_i - x_j| + |y_i - y_j|)/2) \geq 1, i \neq j \quad (14)$$

Criteria for a drone to be receiver in the coexistence link:

A drone cannot be a receiver if it acts as an intermediate node in an already existing sender link otherwise mutual interference will occur. Let us consider three drones D_1, D_2 and D_7 where D_1 is the sender, D_2 will be the receiver of link l_i and D_7 is the intermediate receiver of the link l_j where i is not equal to j. Then, a drone D_4 will act as a receiver from the sender D_8 only if it satisfies the following condition,

$$HD(D_4, D_8) = ((|x_4 - x_8| + |y_4 - y_8|)/2) > 1$$

To prove the above condition, let us first derive the HD of (D_1,D_2), (D_1,D_4), (D_4,D_7) and (D_4,D_8) using below equations,

$$HD(D_1, D_2) = ((|x_1 - x_2| + |y_1 - y_2|)/2) = 1$$
$$HD(D_1, D_4) = ((|x_1 - x_4| + |y_1 - y_4|)/2) = 1$$
$$HD(D_4, D_7) = ((|x_4 - x_7| + |y_4 - y_7|)/2) = 1$$
$$HD(D_4, D_8) = ((|x_4 - x_8| + |y_4 - y_8|)/2) = 1$$

Since the HD(D_4, D_2) =1, both D_4 and D_2 will acts as a receiver at the same time. D_4 cannot act as a sender because the HD(D_1,D_4) =1 does not satisfy the criteria of two senders at the same time.

Hence for a drone to act as a receiver, it should satisfy the following condition given in equation (15).

$$HD(D_i, D_j) = ((|x_i - x_j| + |y_i - y_j|)/2) > 1, i \neq j \quad (15)$$

Where D_i is the sender and D_j is the receiver such that i is not equal to j

Here, two neighbouring drones, for example, D_1 and D_5 are taken for analysis. If both satisfy the above three criteria, then any one of them is excluded from N and the path which begins with their corresponding neighbour is also removed. The remaining paths will be given as the input to A* method. Hence the efficiency of the A* method is improved and the mutual interference problem is also solved.

B. Secured UAV Model

There is a high possibility of attackers in the network to mimic as S-UAV model uses multiple mini UAVs. Also, there is a high chance of integrity and confidentiality loss in exchanging messages due to wireless transmission in the UAV environment. For these two reasons, the proposed S-UAV model focuses on authentication and communication algorithms to make the model more secure.

Algorithm 1 Trusted UAV Authentication

Input: $OTID \leftarrow One\,Time\,ID$
Output: $TID \leftarrow Temporal\,ID$
$MK = MasterKey$ // known only to UI and controller
$SK = SecretKey$
$FK = FrequentKey$
1: Compute Encrypted OTID (E_OTID) using MK.
$E\_OTID = E(OTID, MK)$
2: Decrypt the E_OTID using MK.
$D\_OTID = D(E\_OTID, MK)$
3: Validate it.
if D_OTID == $OTID$ **then**
ID=random()
end if
4: Compute PID and TID using SK and FK.
$PID = E(ID, SK)$
$TID = E(ID, FK)$
5: **return** TID

GPS spoofing, impersonation attack, de-authentication attack, video replay attack and intercept data feed attack have been analysed with respect to security aspects of UAV. The proposed S-UAV model overcomes the above attacks with the help of two cryptographic techniques such as AES and Blowfish.

i). Secure Registration and Authentication: To ensure that the UAV is deployed by the trusted internal user, One Time ID (OTID) is generated by the internal user and encrypted using the Master Key (MK) which is known only to the User Interface (UI) and the controller. This Encrypted OTID (E_OTID) is given to the UAV and it starts the registration and authentication process with the controller. On receiving E_OTID, the controller initiates the decryption process using the MK to ensure that the UAV was deployed by the trusted internal user. The controller maintains two keys: Secret Key (SK) and Frequent Key (FK) which are randomly generated. On successful verification, the controller generates an ID for the UAV and computes the Personal ID (PID) using the SK and Temporal ID (TID) using the FK. The steps for generating TID for trusted UAV is given in Algorithm 1.

PID is used for enclosing the confidential information of the UAV like its current position, traveling path, destination, etc. The controller stores the PID, TID and Previous TID (PTID) as E_OTID for the initial case and current TID for other cases. The controller returns the TID with the authentication complete response to the UAV which begins the communication using this TID. The controller also sends TID and PTID to all the one hop neighbours of the newly registered UAV since the one hop neighbours will be the direct neighbours of the UAV where it begins the communication for routing. After one communication, the TID expires and the UAV sends an ID update request to the controller to change

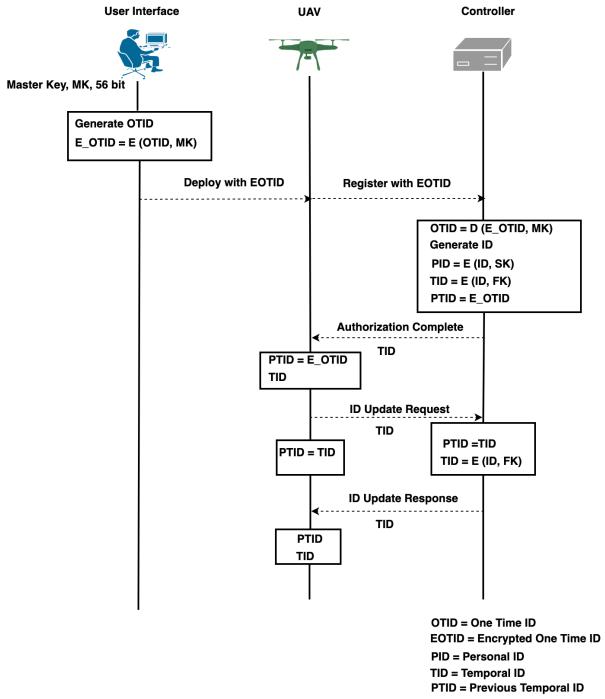

Fig. 4: Secure Registration and Authentication among UAVs

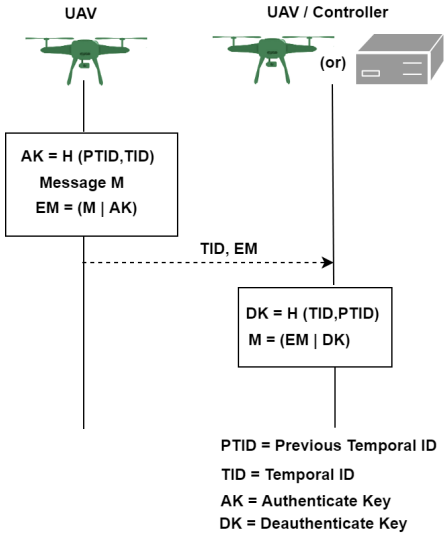

Fig. 5: Secure Communication among UAVs

its TID with the updated FK. The process of secure registration and authentication is illustrated in Fig. 4.

ii). Secure Communication: The process of secure communication is illustrated in Fig. 5. For secure communication, the UAV computes the Authenticated Key (AK) based on PTID and TID. It then encrypts the Message M using the AK and sends the TID and Encrypted Message (EM) to the controller or another UAV for communication. On receiving TID and EM, the controller or other UAV computes the Deauthenticated Key (DK) by using the received TID and existing PTID to get the respective Message M.

For generating AK, a hash function is applied to the TID and PTID. The steps for generating hash value are given in Algorithm 2. This algorithm takes TID, PTID as input and divides them into two 32 bit set. Then two XOR operation is performed, one operation is between first half of TID and last half of PTID and another between the first half of the PTID and the last half of TID. Finally, the hash value is generated by concatenating the results of two XOR operations.

Algorithm 2 Hash Generator

Input: $TID \leftarrow Temporal\ ID$,
$PTID \leftarrow Previous Temporal\ ID$
Output: $H\_Comp \leftarrow Computed\ Hash\ Value$

1: Extract the First 32 bits (FT_32) and Last 32 bits (LT_32) of TID
$FT\_32 = TID[0:31]$
$LT\_32 = TID[32:63]$
2: Extract the First 32 bits (FP_32) and Last 32 bits (LP_32) of PTID
$FP\_32 = PTID[0:31]$
$LP\_32 = PTID[32:63]$
3: Compute hashes $h1$ and $h2$ from the extracted values
$h1 = FT\_32 \oplus LP\_32$
$h2 = FP\_32 \oplus LT\_32$
4: Concatenate the hashes to find the original hash
$H\_Comp = Concatenate(h1, h2)$
5: **return** H_Comp

iii). Secure De-authentication: The process of de-authentication is illustrated in Fig. 6. For the de-authentication request, the UAV sends the TID and AK to the Controller. The controller computes the DK from TID and PTID. If both keys are the same, the controller accepts the de-authentication request and releases the UAV from the network.

C. Secure Encryption and Decryption

There are many cryptographic algorithms like Data Encryption Standard (DES), Secure Hash Algorithm (SHA), Twofish, etc. Each cryptographic algorithm has its weakness in security. For example, Twofish takes more time for encryption and DES takes more processing power. But both blowfish and AES cryptographic techniques have no security weakness so far [28]. So these are the two techniques used for encryption and decryption process and analysis of time complexity for both techniques are shown in the performance analysis section.

In S-UAV model AES and Blowfish are used in the encryption and decryption process of exchanging messages between UAVs and controller. Blowfish is a symmetric key block cipher technique designed by Bruce Schneier which uses the same key for encryption and decryption process. It uses a block size of 64 bits and a key length varying from 32 to 448 bits. AES is a symmetric cryptographic technique

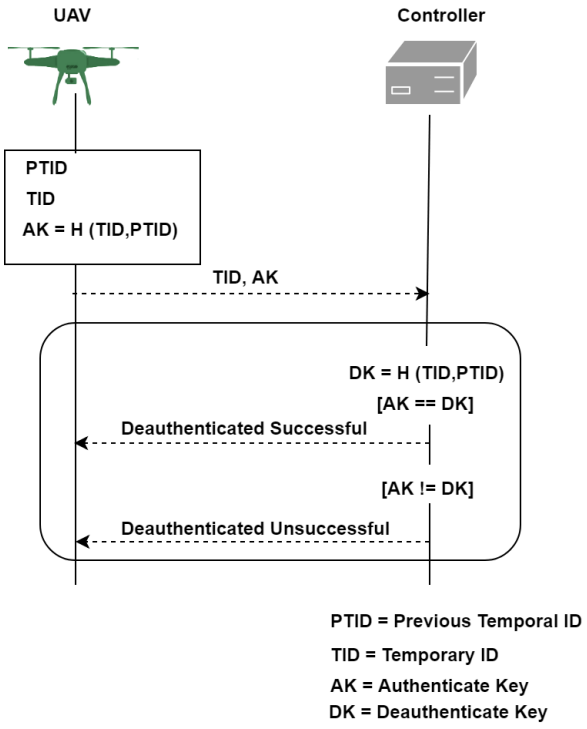

Fig. 6: Secure De-authentication among UAVs

Algorithm 3 Encryption Mechanism

Input: $PT \leftarrow PlainText$,
$k \leftarrow Key\,for\,encryption$
Output: $ET \leftarrow EncryptedText$

1: Find the Remaining Bits (RB) required for PT to equalise the Block Size (B_S) of AES and Blowfish
$RB = B\_S - LENGTH(PT)\%B\_S$
2: Generate random values of size (RB) to get the Padding Bits (PB)
$PB = PACK(random(), RB)$
3: Concatenate PT and PB
$P = Concatenate(PT, PB)$
4: Create a cipher based on the key and mode of operation
$C = Create(K, CBC)$
5: Perform encryption operation using the cipher created
$ET = E(P, C)$
6: **return** ET

with a block size of 128 bit and key sizes of 128,192 and 256 bits. There are four operations performed in each round for the encryption process such as SubBytes, ShiftRows, MixColumns and XorRoundKey. During the decryption process, these operations are performed in a reverse manner.

The input for the encryption mechanism is the Plain Text (PT) and the Encryption Key (K). This key is generated based on the block size of AES and Blowfish. In the first step of the encryption process, the size of the plaintext is compared with the block size of AES or Blowfish. If it is matched, the encryption process continues. Otherwise, Remaining Bits (RB) are padded to the PT to equate

Algorithm 4 Decryption Mechanism

Input: $ET \leftarrow EncryptedText$,
$K \leftarrow Key\,for\,decryption$
Output: $PT \leftarrow PlainText$

1: Create a cipher based on the key and mode of operation.
$C = Create(K, CBC)$
2: Perform decryption operation using the cipher created.
$P = D(ET, C)$
3: Find the Number of Bits (NB) padded in the ET based on Block Size B_S of AES or Blowfish.
$NB = P - LENGTH(P)\%B\_S$
4: Remove the padded bits to obtain the PT
$PT = P[0 : NB]$
5: **return** PT

the block size. For encryption and decryption process, we use the Cipher Block Chaining (CBC) mode wherein each iteration, an XOR operation is performed between current plaintext block and previous ciphertext block. A cipher is created based on the key and mode of operation used. Using the created cipher, the encryption process of AES or Blowfish is completed and Encrypted Text (ET) is obtained. The process of encryption is given in Algorithm 3.

The input to the decryption algorithm is the encrypted text and the decryption key. Initially, a cipher is created based on the key and CBC mode. Using the created cipher, the decryption process of AES or Blowfish is performed on the ET. Following this, the padded bits in the ET are removed to obtain the Plain Text (PT). The process of Decryption is given in Algorithm 4.

V. Performance and Result Analysis

In this section, the simulation analysis of the S-UAV model in a WMN using NS3, mission planner and the security analysis of AES and Blowfish cryptographic techniques are detailed.

A. Efficient use of WMN in UAV

The efficiency of WMN is analysed in different communication environments such as MANET, VANET and UAV.

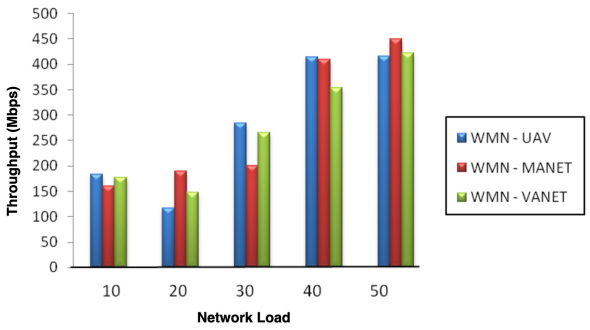

Fig. 7: Throughput vs Number of Devices in WMN Network Load

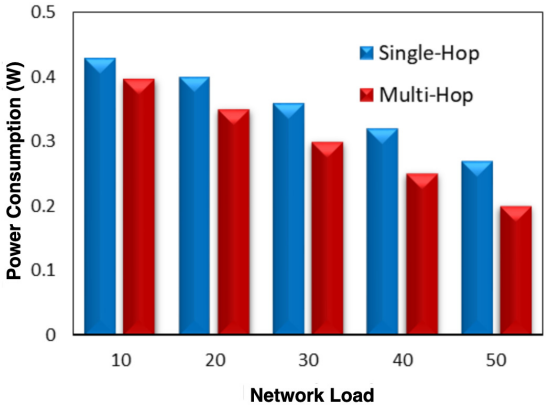

Fig. 8: Power Consumption vs Network Load in WMN

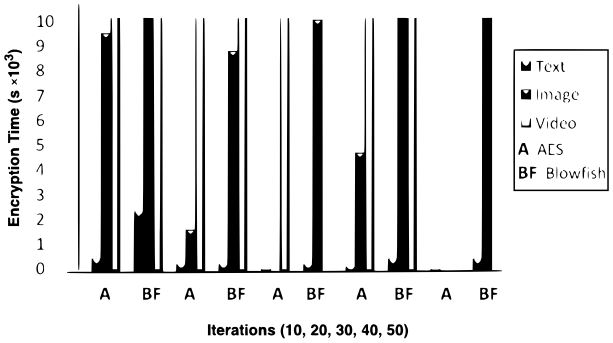

Fig. 9: Encryption Time of AES and Blowfish

The parameters considered for WMN simulation are shown in Table I.

Five groups of UAVs as 10, 20, 30, 40 and 50 are considered for the throughput comparisons with different overheads. WMN is formed for each group based on the location and communicates with the data rate of 150 Mbps. Throughput defines the number of packets transmitting per unit time, and expressed as,

$$Throughput = (RP * |P|)/T \tag{16}$$

Where RP = Total number of received packet
$|P|$ = Packet size
T = Total time.

Fig. 7 shows the throughput variance of using WMN in MANET, VANET and UAV. The throughput of WMN

TABLE I: Simulation Parameters

Parameter	Description
Platform	Ubuntu 18.10
Tool used	NS3 3.27
Simulation Time	100 s
Number of UAVs	10,20,30,40,50
Data Rate	150 Mbps
Monitoring Area	200 km
MAC Layer	IEEE 802.15.4
Simulation Time	2000 s
Network Interface	WirelessPhy
Routing Protocols	LEACH, DSDV

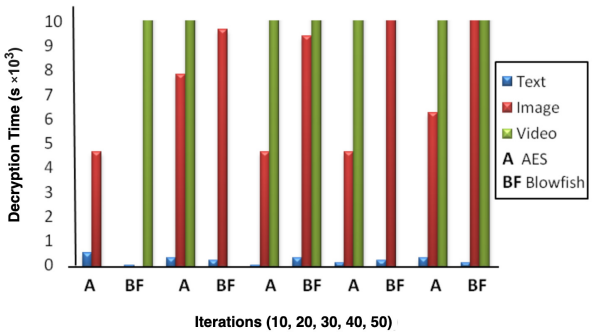

Fig. 10: Decryption Time of AES and Blowfish

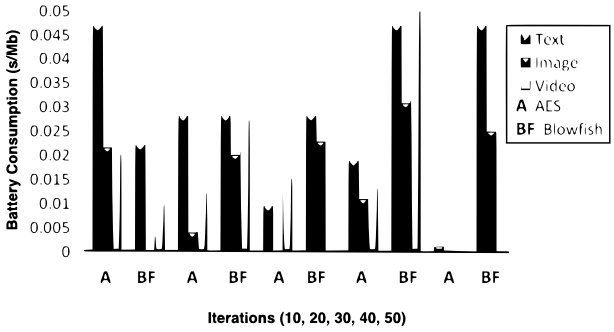

Fig. 11: Battery Consumption of AES and Blowfish

increases by approximately 28% for every 10 iterations in all three environments. In comparison with other environments, the throughput remains almost same in the UAV environment. Thus, WMN is suitable for efficient and secured UAV communication.

As per the proposed S-UAV model, UAV_G_2 gets communicated with the controller with the help of UAV_G_1. Thus, the communication between UAVs and controller is separated in such a way that single-hop communication for UAV_G_1 and multi-hop communication for UAV_G_2 is established. Fig. 8 shows the variation in power consumption during the single hop and multi hop communication between UAVs. The power consumption decreases when there is an increase in network load for both single-hop and multi-hop communication.

B. Analysis of AES and Blowfish in UAV Environment

The cryptographic technique used for encryption and decryption of messages in the UAV environment are AES and blowfish algorithms, and they are implemented in Python. The algorithms are analysed with three different input types as text, image and video of size 11KB, 425 KB and 3055 KB. AES and Blowfish techniques are computed for 50 iteration and average encryption time, decryption time and battery consumption are plotted as shown in Fig. 9, 10 and 11.

The computation overhead is examined in terms of encryption and decryption time, as shown in Fig. 9 and Fig. 10. Encryption and decryption time depend on the block

TABLE II: Attacks Comparison

Attack name	Proposed S-UAV model	Challa *et al.* [29]	Turkanović *et al.* [30]	Wazid *et al.* [28]
GPS Spoofing	✔	✗	✗	✗
De-authentication attack	✔	✗	✗	✗
Intercept data feed attack	✔	✗	✗	✗
Video replay attack	✔	✔	✔	✔
Impersonation attack	✔	✔	✔	✔

size of plaintext, size of the key and type of mode used. When encryption or decryption is performed for the first time, the entire process is executed for all bits and the results are cached. An encrypted text from the cache will be used from the next iteration, leading to a decrease in encryption or decryption computation time. For every 10 iterations, AES and Blowfish decrease encryption time up to 85% and 57%, and AES decreases decryption time up to 40.6%, while Blowfish remains relatively constant. Both encryption and decryption time is comparatively less in AES and thus meets the requirements for real world application.

Battery consumption acts as a critical parameter for UAVs, UAV uses its battery power to perform communication, authorization, computation, etc. Thus a cryptographic algorithm with low battery power requirements is required. On comparing AES and Blowfish, AES takes less power to perform the computation. On the other hand, Blowfish uses a longer key for the process hence hacking the key value is difficult.

C. Security Analysis

Dolev-Yao threat model in which a communication channel is public and endpoint entities such as UAVs are considered untrustworthy. In such a model, an attacker can eavesdrop, delete or modify the exchanged messages. Thus the proposed S-UAV model is compared with the authentication and communication model proposed by Challa *et al.* in [29], Turkanović *et al.* in [30], Wazid *et al.* in [28] and the attacks are compared in Table II.

FK is updated periodically by the controller and the probability of finding the SK is negligible. Thus, the PID of the UAV is never compromised and therefore confidential information of UAV is always maintained.

The attacker captures the UAV and hacks its TID. Still the attacker cannot communicate with other UAVs or controller because the attackers cannot find the AK that was computed for communication. Therefore impersonation and de-authentication requests from the attacker are rejected by the controller. Thus the GPS Spoofing in which the attacker changes the UAV path, Video replay attack and impersonation attack where the attacker intercepts the UAV fails due to the generation of the strong authentication key.

VI. Conclusion

In this paper, the proposed S-UAV model with efficient WMN formation reduces the processing time. The model uses the A* algorithm to find the shortest path, which overcomes the infinite loop problem in BFS and also takes half the time for route discovery when compared with the Dijkstra algorithm. The registration and authentication using EOTID ensures that the UAV is launched by a trusted user. Thus the overall security process overcomes GPS Spoofing, de-authentication, intercept data feed, video replay and impersonation attacks.

Acknowledgement

This Publication is an outcome of the R&D work undertaken in the project under the Visvesvaraya PhD Scheme of Ministry of Electronics Information Technology, Government of India, being implemented by Digital India Corporation (formerly Media Lab Asia).

References

[1] Yanmaz E, Yahyanejad S, Rinner B, Hellwagner H and Bettstetter C, "Drone networks: Communications, coordination, and sensing", *Ad Hoc Networks*, pp.1-15, 2018.

[2] Gunasekaran Raja, Sudha Anbalagan, Vikraman Sathiya Narayanan, Srinivas Jayaram and A. Ganapathisubramaniyan, "Inter-UAV Collision Avoidance using Deep-Q-Learning in Flocking Environment," *IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York City, NY, USA, pp. 1089-1095, 2019.

[3] Singh P.J, de Silva R and Seher I, "Comparison of communication protocols for UAVs and VANETs", *IEEE International Conference on Computing, Communication and Automation (ICCCA)*, pp. 616-619, Apr. 2016.

[4] Hong T.C, Kang K, Lim K and Ahn J.Y, "Network architecture for control and non-payload communication of UAV", *IEEE International Conference on Information and Communication Technology Convergence (ICTC)* , pp. 762-764, Oct. 2016.

[5] Rosati S, Kruzelecki K, Traynard L and Rimoldi B, "Speed-aware routing for UAV ad-hoc networks", *IEEE Globecom Workshops(GC Wkshps)*, pp. 1367-1373, Dec. 2013.

[6] Rajakumar Arul, Gunasekaran Raja, Ali Kashif Bashir, Junaid Chaudhry and Amjad Ali, "A Console GRID leveraged Authentication and Key Agreement Mechanism for LTE/SAE", *IEEE Transactions on Industrial Informatics,* vol. 14, no. 6, pp. 2677–2689, Jun. 2018.

[7] Sheeba Backia Marry Bhaskaran, Gunasekaran Raja, Ali Kashif Bashir and Masayuki Murata, "QoS-aware frequency-based 4G+ relative authentication model for next generation LTE and its dependent public safety networks", *IEEE Access,* vol. 5, pp. 21977–21991, Nov. 2017.

[8] Sahingoz O.K, "Networking models in flying ad-hoc networks (FANETs): Concepts and challenges", *Journal of Intelligent Robotic Systems*, vol. 74, issue 1-2, pp.513-527, Apr. 2014.

[9] D. Zhang, Y. Liu, L. Dai, A. K. Bashir, A. Nallanathan and B. Shim, "Performance Analysis of FD-NOMA based Decentralized V2X Systems", *IEEE Transactions on Communications*. vol. 67, no. 7, pp. 5024-5036, 2019.

[10] Catalina Aranzazu Suescun and Mihaela, "Unmanned Aerial Vehicle Networking Protocols", *LACCEI International Multi-Conference for Engineering, Education, and Technology: Engineering Innovations for Global Sustainability*, DOI: 10.18687/LACCEI2016.1.S.078, Jan. 2016.

[11] Hayat S, Yanmaz E and Muzaffar R, "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint", *IEEE Communications Surveys and Tutorials*, no. 4, pp.2624-2661, 2016.

[12] Marcus M, "Spectrum policy challenges of UAV/drones [spectrum policy and regulatory issues]", *IEEE Wireless Communications*, vol. 21, issue 5, pp.8-9, Oct. 2014.

[13] S.A. Hussain, M. Iqbal, A. Saeed, I. Raza, H. Raza, A. Ali, A.K. Bashir and A. Baig, "An Efficient Channel Access Scheme for Vehicular Ad hoc Networks", *Mobile Information Systems, Hindawi*, vol. 2017, pp. 1-10, 2017.

[14] Boychev I.Z, "Research algorithms to optimize the drone route used for security", *IEEE International Scientific Conference Electronics-ET*, pp. 1-4, Sep. 2018.

[15] Ramkumar Jayaraman, Gunasekaran Raja, Ali Kashif Bashir, Chauhdary Sajjad Hussain, Ali Hassan and Mohammad A. Alqarni, "Interference Mitigation Based on Radio Aware Channel Assignment for Wireless Mesh Networks", *Wireless Personal Communications,* DOI: 10.1007/s11277-018-5776-4, 2018.

[16] Cui Q, Liu P, Wang J and Yu J, "Brief analysis of drone swarms communication", *IEEE International Conference on Unmanned Systems (ICUS)*,pp. 463-466, 2017.

[17] Kumaravel Krishnan K, Renugadevi R, Marimuthu A, "A Study On Protocols In Wireless Mesh Network", *International Journal of Computer Science Engineering Technology (IJCSET)*, vol. 6, pp. 413-415, Jul. 2015.

[18] Nayyar A, "Flying Adhoc Network (FANETs): Simulation Based Performance Comparison of Routing Protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP", *International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, pp. 1-9, Aug. 2018.

[19] Krishna C.L. and Murphy R.R, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles", *IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pp. 194-199, Oct. 2017.

[20] Vattapparamban E, Güvenc I, Yurekli A.I, Akkaya K and Uluagac S, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety", *IEEE International Wireless Communications and Mobile computing Conference (IWCMC)*, pp. 216-221, Sep. 2016.

[21] M. A. Javed, N. S. Nafi, S. Basheer, M. A. Bivi and A. K. Bashir, "Fog-Assisted Cooperative Protocol for Traffic Message Transmission in Vehicular Networks", *IEEE Access*, vol. 7, pp. 166148-166156, 2019.

[22] R. Abbasi, H. Hassan, W. Ahmed, G. Rehman; N.M. F. Qureshi, B. Luo and A. K. Bashir, "Generalized PVO based Dynamic Block Reversible Data Hiding for Secure Transmission Using Firefly Algorithm", *Transactions on Emerging Telecommunications Technologies, Wiley*, DOI: 10.1002/ett.3680, 2019.

[23] Yu J, Cho B.M, Park K.J. and Kim H, "Simultaneous Attack on Drone and GCS in UAV Systems", *International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 5-7, Jul. 2018.

[24] Cheon J.H, Han K, Hong S.M, Kim H.J, Kim J, Kim S, Seo H, Shim H and Song Y, "Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption", *IEEE Access*, pp.24325-24339, 2018.

[25] Diamond P, "Detection, mitigation, recovery of GPS based assured timing critical infrastructure when under attack by spoofing or jamming", *IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1-4, Apr. 2017.

[26] G. Raja, S. Anbalagan, G. Vijayaraghavan, P. Dhanasekaran, Y. D. Al-Otaibi and A. K. Bashir, "Energy-Efficient End-to-End Security for Software Defined Vehicular Networks," *IEEE Transactions on Industrial Informatics*, DOI: 10.1109/TII.2020.3012166, 2020.

[27] Gunasekaran Raja, Aishwarya Ganapathisubramaniyan, Madhumitha Sri Selvakumar, Thiruveni Ayyarappan and Karthikeyan Mahadevan, "Cognitive Intelligent Transportation System for Smart Cities", *Proc. 10 th IEEE International Conference on Advanced Computing (ICoAC), Chennai*, pp. 146–152 Dec. 2018.

[28] Wazid M, Das A.K, Kumar N, Vasilakos A.V and Rodrigues J.J, "Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment", *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572-3584, 2019.

[29] Challa S, Wazid M, Das A.K, Kumar N, Reddy A.G, Yoon E.J and Yoo K.Y, "Secure signature-based authenticated key establishment scheme for future IoT applications", *IEEE Access*, pp.3028-3043, 2017.

[30] Turkanović M, Brumen B and Hölbl M, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion", *Ad Hoc Networks*, pp.96-112, 2014.